IoT時代のセーフティとセキュリティ

「IoT時代のセーフティ設計技術解説」

2015年3月30日

サプライチェーンにおける品質の見える化WG委員
株式会社ヴィッツ 執行役員　機能安全開発部　部長
株式会社アトリエ 取締役
森川　聡久

本日の内容

IoT時代のシステム開発において必要となるセーフティ設計技術について、機能安全を中心に一部本質安全を含めて、実施すべき開発手順・分析手法・対処法などについて解説します。

＜目次＞

0. 弊社の機能安全実績のご紹介
1. IoT時代にも必要となる(機能)安全への対応
2. セーフティの分析・設計技術（H&R）
3. セーフティの分析・設計技術（機能安全）
4. セーフティの立証技術
5. ガイドブックのご紹介

0. 弊社の機能安全実績のご紹介

IEC61508, ISO26262 機能安全プロセス認証取得

株式会社 ヴィッツ

【国内初】2010年4月：
機能安全規格 **IEC61508 SIL3対応** ソフトウェアプロセス認証を取得

【世界初】2012年3月： ※世界初は当社調べの限り
自動車 機能安全規格 **ISO26262 ASIL-D（最高レベル）対応** ソフトウェアプロセス認証を4社同時取得（東芝 2社, パナソニック,ヴィッツ）
その後、アイシン2社、自動車関連企業2社の取得支援成功！

プロセス認証取得企業は、国内外で増加傾向にあり

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE
No. Q4B 10 04 73778 002

Holder of Certificate: Witz Corporation
Shirakawa 2nd BLDG.
13-1, SAKAE 2-CHOME, NAKA-KU
NAGOYA
460-0008 JAPAN

Factory(ies): Witz Corporation
Shirakawa 2nd BLDG., 13-1, SAKAE 2-CHOME, NAKA-KU, NAGOYA, 460-0008 JAPAN

Certification Mark: TÜV SÜD

Scope of Certificate: Software Development Process

Applied Standard(s): Software Development Process including Overall Safety Lifecycle Requirements and Functional Safety Management according to
IEC 61508-1:1998 (SIL 1-3)
IEC 61508-2:2000 (as applicable)
IEC 61508-3:1998 (SIL 1-3)
IEC 61508-4:1998 (as applicable)

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: WN83079T
Valid until: 2013-04-18

Date, 2010-04-22 (Peter Weiss)
Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstrasse 65 · 80339 München · Germany

IEC61508:1998

ズームイン (Ctrl++)

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE
No. Q4B 12 03 73778 001

Holder of Certificate: Witz Corporation
Shirakawa 2nd BLDG.
13-1, SAKAE 2-CHOME, NAKA-KU
NAGOYA
460-0008 JAPAN

Factory(ies): Witz Corporation
Shirakawa 2nd BLDG., 13-1, SAKAE 2-CHOME, NAKA-KU, NAGOYA, 460-0008 JAPAN

Certification Mark: TÜV SÜD

Scope of Certificate: Software Development Process

Applied Standard(s): Software Development Process including Overall Safety Lifecycle Requirements and Functional Safety Management according to
IEC 61508-1:2010 (SIL 1-3)
IEC 61508-3:2010 (SIL 1-3)
ISO 26262-2:2011 (ASIL A-D)
ISO 26262-6:2011 (ASIL A-D)
The report WN84228C is a mandatory part of this certificate.

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: WN84228C
Valid until: 2015-03-14

Date, 2012-03-16 (Guido Neumann)
Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

IEC61508:2010, ISO26262:2011

安全コンセプトレポート取得成功!!

・平成22年度～24年度：3年間の活動
・軽くて厳格な保護が可能な「ParOS」を、パーティションOSの決定版として、仕様策定から実装まで研究開発した。
・上流レベルの「技術安全コンセプト」を国際認証機関TUV SUDにアセスメントしていただき、「complete評価」をいただいた。 ※アセスメント ≠ コンサル

Review Report

of the

Partition OS Safety Concept

Applicant
Witz Incorporation
Shirakawa 2nd Bldg. 2F, 7F, 13-1
Sakae 2-Chome
Naka-ku
460-0008 Nagoya
Japan

Manufacturer
Witz Incorporation
Same as above

Report no. WN84129T
Revision: 2.0, Date 18.01.2013

Test and Certification body

TÜV SÜD Rail GmbH
Generic Safety Systems
Barthstraße 16
D-80339 Munich

Page 1 of 16

This technical report may be represented only in complete wording. The use for promotion needs written permission. It contains the result of a unique investigation of the product being tested and places no generally valid judgment about characteristics out of the running fabrication. Official translations of this technical report are to be authorized by the test and certification agency.

6 Summary

The available documentation of Witz Inc. is complete with respect to the concept of the TOE as defined in chapter 1.

The safety manual has to be completed in the detailed phases of a specific project depending on the project specific regulation of deliverables by Witz Inc. This includes requirements resulting from the fact that Witz Inc. makes it mandatory to order the Board Support package development to Witz Inc. The resulting "final" safety manual shall be reviewed and checked to achieve precise and accurate instructions for the user of ParOS.

The requirements of IEC 61508 2nd Edition are met. The results and recommendations can be used to execute the detailed development phase and documentation for PartitionOS.

i.V. Guido Neumann
Technical Certifier

i.A. Sylvia Waldhausen
Expert Functional Safety

※ParOS安全コンセプトレポートからの抜粋

主な機能安全支援実績

＜機能安全対応コスト＞
数億円～数十億円、数年間

弊社の知見投入

わからないから莫大なコストがかかる

期間半減!! 費用半減!! を目指した支援

他にも
鉄道、ガス機器、農業機械
サービスロボット、
などの対応実績もあるよ♪

支援企業実績: 41 社　支援プロジェクト実績: 71 プロジェクト

2014年12月現在

支援項目	A社	B社	C社	D社	E社	F社	G社	H社	I社	J社	K社	L社	M社	N社	O社	P社	Q社	R社	S社	T社	U社	V社	W社	X社	Y社	Z社	a社	b社	c社	d社	e社	f社	g社	h社	i社	j社	k社	l社	m社	n社	o社
①機能安全プロセス、安全計画の構築	●	●	●			●	●	●	●	●					●	●			●		●	●		●	●	●	●	●	●	●	●	●							●		
②技術安全コンセプトの構築	●		●			●				●		●			●		●	●	●		●			●				●		●	●	●				●		●	●		●
③FMEDA安全分析＆故障率算出評価	●	●								●								●			●																				
④機能安全開発受託	●	●				●				●				●	●		●			●						●						●				●					
⑤機能安全第3者検証・監査	●	●				●	●	●	●	●				●	●	●			●	●	●									●		●				●		●			
⑥開発ツールの機能安全対応		●									●		●																	●						●					
トレーサビリティ管理ツール導入		●				●	●			●		●							●								●								●						
機能安全対応RTOS導入															●								●																		
ノウハウコンテンツ導入				●	●	●	●	●	●	●			●									●			●												●				
機能安全教育						●						●				●	●		●			●					●			●			●	●			●			●	
機能安全規格解説(**無料コンサル※**)	●	●	●			●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●		●	●	●	●	●	●		●	●				●		●	●		●
機能安全認証取得支援	●					●	●	●	●	●									●	●	●	●		●	●											●					
システム、ECU対応	●	●	●							●	●	●	●	●	●		●	●	●	●	●			●		●	●	●				●	●	●				●	●	●	
ハードウェア対応	●	●								●	●			●	●				●		●			●			●	●			●		●	●					●	●	
ソフトウェア対応	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●		●	●	●	●	●	●	●	●	●		●	●	●	●		●		●	●	●
IEC 61508	●	●		●	●	●	●	●	●	●		●											●																		
ISO 26262			●	●		●	●	●	●	●	●	●	●	●	●	●	●		●			●			●	●	●		●	●	●	●	●	●	●		●	●	●	●	●
ISO 13849		●								●								●										●								●					
その他の機能安全規格	●			●		●				●										●	●			●				●								●					

※無料コンサルは、まとまった開発・作業委託をいただいた場合に対応しております。

弊社の機能安全実績の特徴

- ①多分野・多企業への**実開発支援**によるノウハウの蓄積
- ②欧州認証機関との豊富な活動経験
  - **延べ10プロジェクト以上、70回以上、500h以上のミーティング経験**

Review Report

of the

Partition OS Safety Concept

Applicant

Witz Incorporation
Shirakawa 2nd Bldg. 2F, 7F, 13-1
Sakae 2-Chome
Naka-ku
460-0008 Nagoya
Japan

Manufacturer

Witz Incorporation
Same as above

Report no. WN84129T
Revision: 2.0, Date 18.01.2013

Test and Certification body

TÜV SÜD Rail GmbH
Generic Safety Systems
Barthstraße 16
D-80339 Munich

Page 1 of 16

This technical report may be represented only in complete wording. The use for promotion needs written permission. It contains the result of a unique investigation of the product being tested and places no generally valid judgment about characteristics out of the running fabrication. Official translations of this technical report are to be authorized by the test and certification agency.

6 Summary

The available documentation of Witz Inc. is complete with respect to the concept of the TOE as defined in chapter 1.

The safety manual has to be completed in the detailed phases of a specific project depending on the project specific regulation of deliverables by Witz Inc. This includes requirements resulting from the fact that Witz Inc. makes it mandatory to order the Board Support package development to Witz Inc. The resulting "final" safety manual shall be reviewed and checked to achieve precise and accurate instructions for the user of ParOS.

The requirements of IEC 61508 2nd Edition are met. The results and recommendations can be used to execute the detailed development phase and documentation for PartitionOS.

i.V. Guido Neumann
Technical Certifier

i.A. Sylvia Waldhausen
Expert Functional Safety

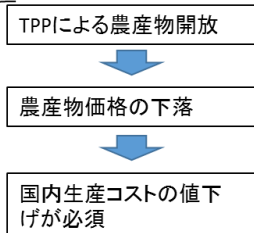
⇒ グローバル基準に対する豊富な実践経験

- **③Safety（機能安全） & Security（組込みセキュリティ）**
  - 主な組込みセキュリティ活動
    - 重要生活機器連携セキュリティ協議会（CCDS）
    - サポイン3件
    - JASPAR 情報セキュリティ実証WG

セキュリティ,パーティションOS,AUTOSAR,MBD

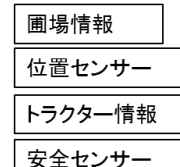
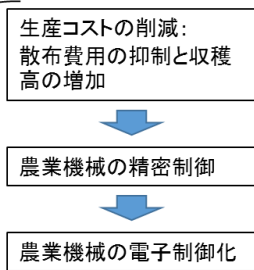
農機の標準通信規格・機能安全対応を促進する基盤ソフトの整備

平成26年度採択サポイン「農業機械のさらなる高度化と海外進出に資する次世代電子制御ソフトウェア基盤の開発」

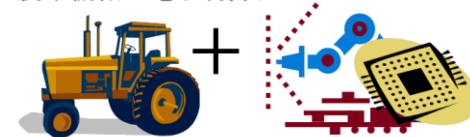
農業の背景と課題

- TPPによる農産物開放
- 農産物価格の下落
- 国内生産コストの値下げが必須
- 労働コストの削減：⇒トラクタ等の自律化

農業機械への要望

- 生産コストの削減：散布費用の抑制と収穫高の増加
- 農業機械の精密制御
- 農業機械の電子制御化

圃場情報 / 位置センサー / トラクター情報 / 安全センサー

既存農業機械

既存農業機械は労働支援のみ

農業機械の電子制御化

電子制御化された次世代農業機械による精密かつ安全な作業は、生産コスト削減のための有効な方法

Smart Safety Agriculture

電子制御化の課題

- 【低コスト化】簡便なソフトウェア開発技術
- 【標準準拠】通信制御・機能安全

農業機械の課題

本研究範囲

- 自動車技術の活用
- 簡易設計ツールの開発
- ISO-BUSの活用
- ISO 25119対応

農業IT化の促進

本研究成果による貢献

Smart Safety Agriculture

- 国内生産コストの削減
- 農業機械の安全担保
- 農業機械企業の国際競争力向上実現

欧米農機メーカー

農機用次世代ソフト基盤

国内農機メーカー

標準通信規格 ISO 11783 / ISOBUS

2000年前後から対応

10年behind

ISOBUS・機能安全対応
ソフト基盤で競争力強化を支援

機能安全規格 ISO 25119

2010年頃から対応開始

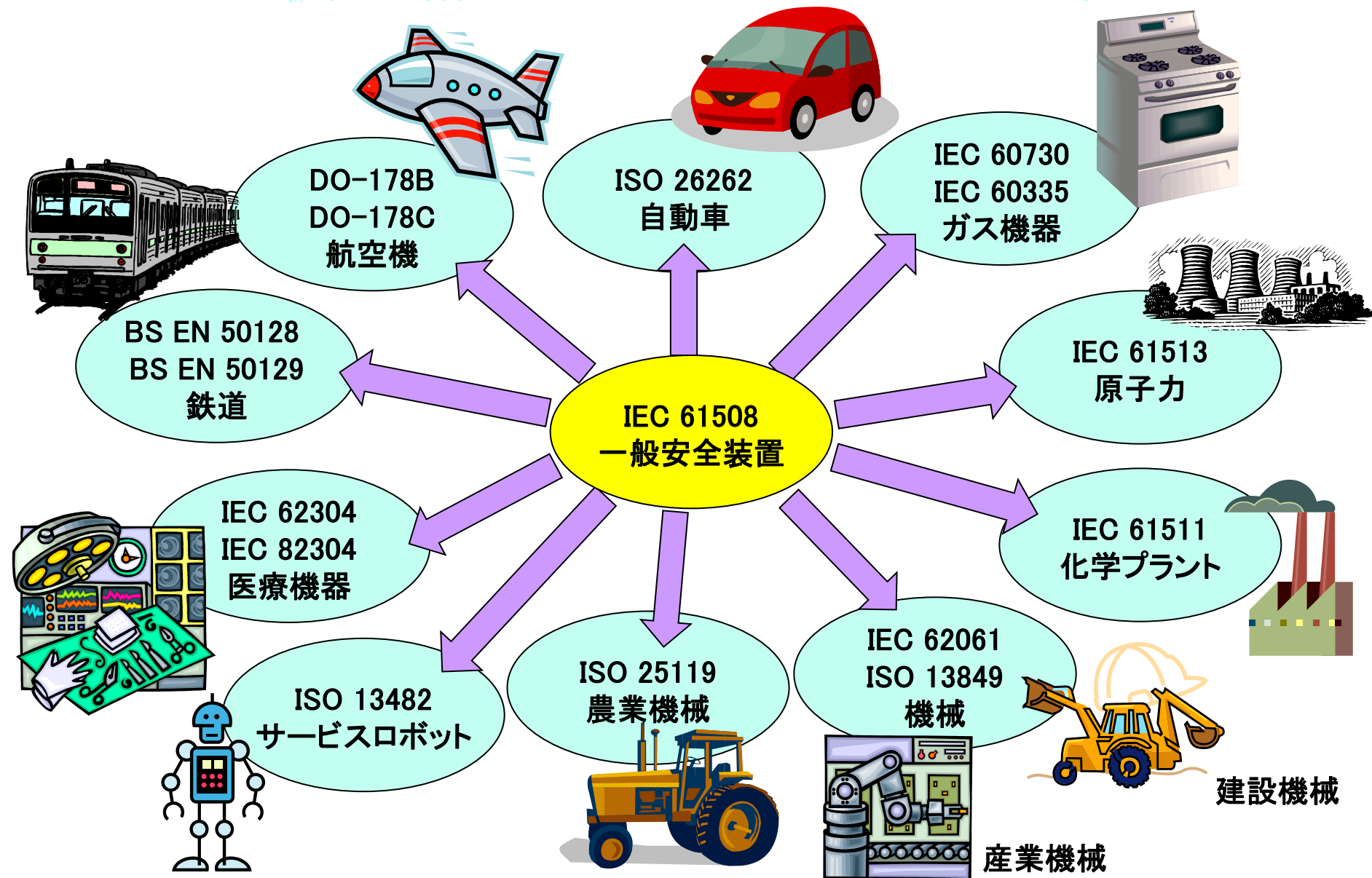
5年behind

機能安全設計への形式手法適用、GSN・SafeMLの利用など予定

1. IoT時代にも必要となる（機能）安全への対応

さまざまな産業ドメインで対応必須化する機能安全

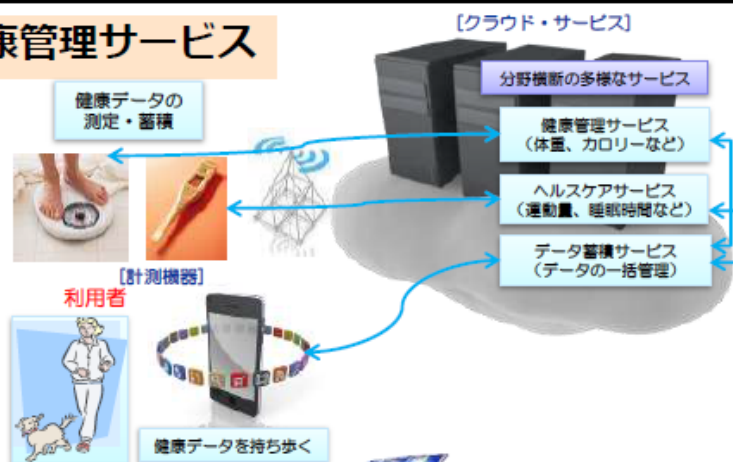
株式会社 ヴィッツ

IoT時代のセーフティの必要性

ネットワーク連携によりシステムは益々複雑に ⇒ セーフティ対応必須

指摘された課題例：ソフトウェア連携イメージ

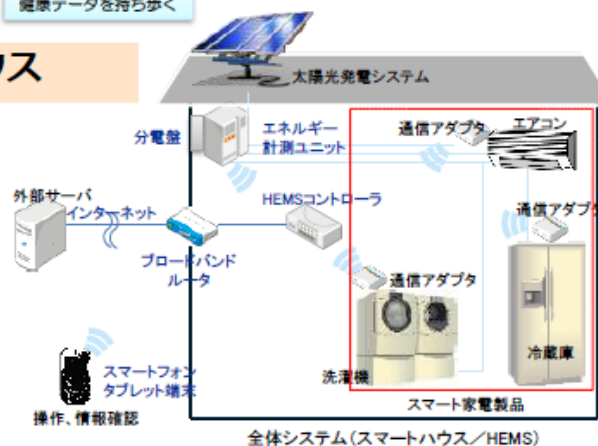
SEC Software Reliability Enhancement Center

例１：健康管理サービス

［クラウド・サービス］
分野横断の多様なサービス
健康管理サービス（体重、カロリーなど）
ヘルスケアサービス（運動量、睡眠時間など）
データ蓄積サービス（データの一括管理）
健康データの測定・蓄積
［計測機器］
利用者
健康データを持ち歩く

品質、安全性、セキュリティ基準等が異なる製品間の相互接続が拡大

接続可否判断と相互につながるソフトウェア間の品質やセキュリティ確保が重要

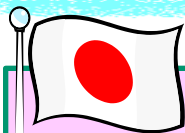
例２：スマートハウス

太陽光発電システム
分電盤
エネルギー計測ユニット
通信アダプタ
エアコン
外部サーバ
インターネット
HEMSコントローラ
ブロードバンドルータ
通信アダプタ
通信アダプタ
冷蔵庫
洗濯機
スマートフォン タブレット端末
操作、情報確認
スマート家電製品
全体システム（スマートハウス／HEMS）

利用者が製品やサービスを組み合わせて利用

利用者が連携時のリスクを十分に理解できていない。

IPA Software Reliability Enhancement Center 11

抜粋元：サプライチェーン事業者の取組み事項整理 Safety & Security Part 1（2014年7月17日）

従来開発と機能安全開発の大きな違い

従来開発

①壊れないモノ作り

・自己努力によって**壊れにくいもの**、バグゼロが目標

・匠の技術で作られた**高信頼性部品**を使用

②日本流開発スタイル

・担当者間の"すり合わせ開発"で、効率的に開発を進行

・開発文書の出来栄えは**不十分(必要最小限)**

安全性強化

開発スタイルへ 不慣れな

機能安全開発

①壊れても安全なモノ作り

・高品質の**証拠を積み重ねた開発**によってバグゼロが目標

・**万が一構成部品が故障しても危険にならない「仕組み」**が必要

②安全説明力のある開発

・PL訴訟時に**安全を客観的に説明できる開発文書**の作成や**エビデンス**が必要

組込みシステムの複雑化による事故多発への対応として「実の安全性向上」と「PL訴訟対策」のため、機能安全は生まれた

機能安全対応製品の実現ステップ

製品個別対応

組織対応

機能安全対応製品

機能安全開発・評価

機能安全開発
・システム開発・V&V
・HW開発・V&V
・SW開発・V&V
・回路図の安全分析
・SWアーキの安全分析

機能安全評価
・SIL/ASIL故障率評価
・機能安全監査

コンセプト開発

安全計画
・FSMプラン
・V&Vプラン
・調達（ツール・外注）

安全目標の定義
・H&R分析
・目標SIL/ASIL決定

技術安全コンセプト構築
・安全コンセプト
・安全要求仕様書
・安全マニュアル
・システム安全分析

機能安全管理システムの構築（IEC 61508, ISO 26262, ISO 13849, etc）

既存開発とのギャップ診断

プロセス構築
・規定
・ガイドライン
・テンプレート
・チェックリスト

×

・システム
・HW
・SW

プロセス改善・定着

品質管理システムの構築（CMMI, A-SPICE）

プロセス構築
・規定
・ガイドライン
・テンプレート
・チェックリスト

×

・システム
・HW
・SW

プロセス改善・定着

不明確な文書化基準

どう書けば「簡潔」と言えるのか？

＜内容＞
- ・正確
- ・簡潔
- ・理解容易性
- ・明白な構成
- ・保全性
- ・内容が妥当

どう書けば「理解容易」なのか？

どう書けば「明白」と言えるのか？

規格書の要求事項は非常に曖昧。合格基準がわからない・・・。
そこで、「PL訴訟対策」という、もう1つの目的が重要になってくる。

注）規格書には「PL訴訟対策のため」とは載っていないので、
「機能安全規格要求」と「PL訴訟対策」は別要求なのです。
*しかし、「PL訴訟対策のために機能安全に適合するのだから、**PL訴訟で通用するエビデンスでなければならない**」ことが、「暗黙の要求事項」になっている。*

文書化要件の重要ポイント

- 機能安全が求めること　満たせば ⇒ **安全性を説明可能**
  - **完全性・一貫性**
    - 開発・管理・運用に必要な情報が全て記載/記録されていること
    - 過不足・矛盾がない
    - あらゆる観点での検証(Verification)を実施して確認されていること
  - **再現性 ＋ 客観性**
    - 再現/再検証できること（他者でも、数年後でも）

⇒ 再現できない内容だと・・・
・安全であることを、客観的に確認できない
・後の不具合発生時に、問題原因を追究できない

  - **可読性 ＋ 客観性**
    - 同意の理解ができること（他者が見ても、数年後に見ても）

⇒ 誤解するような内容だと・・・
・関連モジュールに不具合混入の恐れ
・後のメンテで誤修正の恐れ

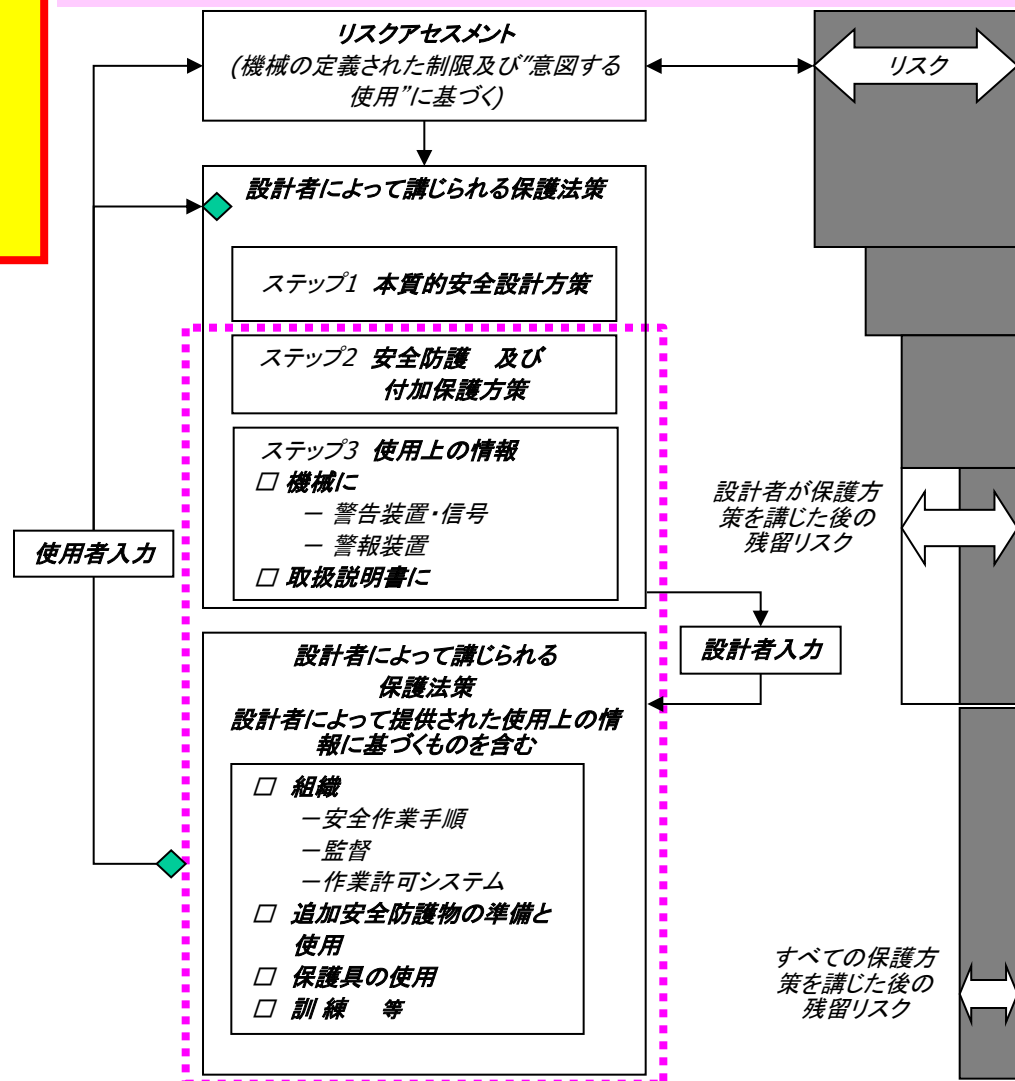
PL訴訟で通用するには、再現性・客観性・可読性 が重要!!

機能安全だけでは安全なモノは作れない!!

株式会社 ヴィッツ

機能安全は「安全策の一種」にすぎない！
さまざまな対策を打って
やっと「安全」なものができる。

- リスク低減プロセス（3ステップメソッド）
  1. 本質的安全設計
  2. 安全防護、付加保護方策（機能安全）
  3. 使用上の情報
- 開発だけでなく、運用時の対応も重要！

まずは「機械安全」 *ISO12100（JIS B 9700）: 機械類の安全性一設計のための一般原則ーリスクアセスメント及びリスク低減* が重要!!

JIS B 9700-1 図1

2. セーフティの分析・設計技術（H&R）

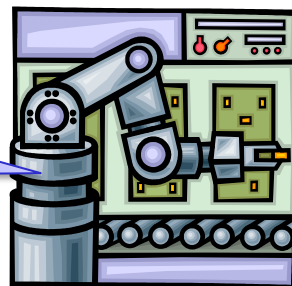
H&R vs 安全分析

- ハザード&リスク分析(H&R) ≒ ISO12100
  - ハザード(危険事象)を抽出し、
    - 機能安全では「万が一故障した場合の誤動作」も想定
  - リスクを評価し、
    - 機能安全では「SIL/ASIL」などが決定
  - 安全策を検討する。

- 安全分析(機能安全)
  - 前提:電気系部位の故障対策(安全設計)が検討済
  - 電気系部位について、故障しても危険にならないことを確認する。

具体的イメージ例

<H&R>

①ハザード
制御が暴走したら危険!!
②リスク評価
SIL2

※注）非常停止ボタンだけで十分安全になるかは不明

STOP

③安全策
「非常停止ボタン」を付けよう!!

<従来設計（機能実現）>

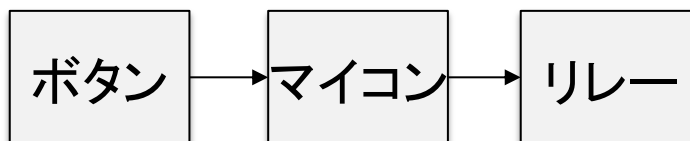
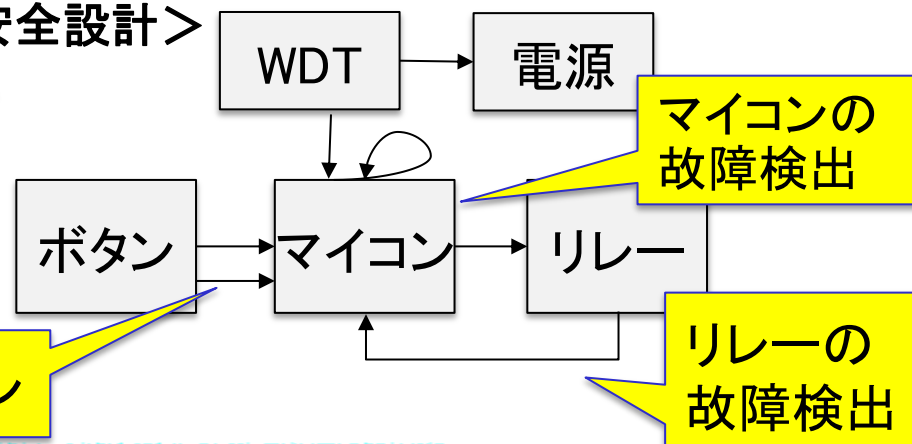
ボタン → マイコン → リレー

④安全要求の定義
「非常停止ボタン押下時に確実に停止すること（SIL2）」

<安全設計>

WDT → 電源

ボタン → マイコン → リレー

マイコンの故障検出

リレーの故障検出

2重接点ボタン

<安全分析>

SIL2を満たす安全設計であることを確認する。

H&Rに必要な情報

株式会社ヴィッツ

※参照：ISO12100

機械類の説明に関連する事項

- 使用者の仕様
- 想定される機械類の仕様
  - 全ライフサイクルの説明
  - 設計図面
  - 動力源及び供給方法
  - 以前設計した類似の関連書類
  - 使用上の情報

法規制、規格及び他の適用可能な文書に関する事項

- 適用可能な法規制
- 関連する規格
- 関連する技術仕様
- 関連する安全データシート

使用経験に関する事項

- 事故履歴
- インシデント履歴
- 機能不良履歴
- エミッションの履歴
- 使用された化学物質の履歴
- 加工される材料による健康被害の履歴

関連する人間工学原則

- 人と機械のインタラクション（操作ミスを誘発するようなもの【例】ボタン配置、ハンドル操作方向など）

↓

リスク分析（H&R）

機械類の制限の決定(H&R)

株式会社 ヴィッツ
※参照:ISO12100

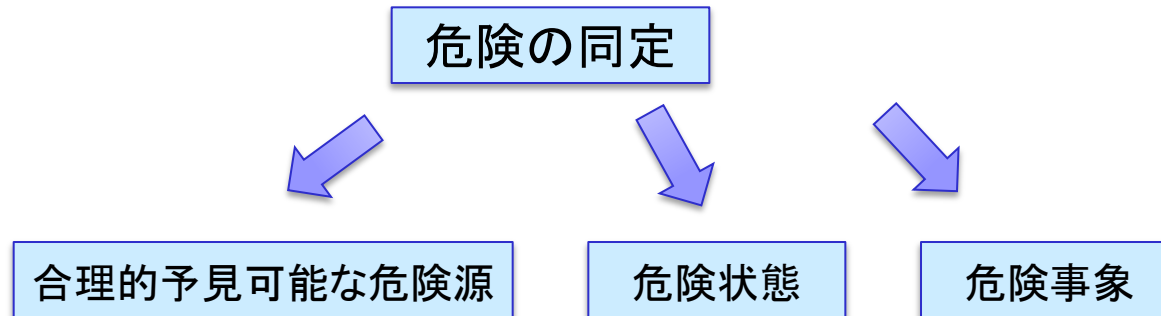
- 『機械が使用される目的・条件』を明確化するため、機械類の制限の決定を行う。
- 機械類の制限の例(JIS9700:2013/5.3項)を以下に示す。

有効期限は何年か？
どういう目的で使用される？
使用者は、どういった条件を満たす必要があるか？
設置のための条件は何か？

機械が使用される目的・条件

危険源の同定(H&R)

※参照:ISO12100

- 機械のライフサイクルの全局面(運搬、組立て及び設置、コミッショニング(立ち上げ、検収引渡し、移管)、使用、分解、利用停止、及び廃棄処分)における、合理的に予見可能な危険源、危険状態及び/又は危険事象を系統的に同定する。

- 危険源の同定に用いられる『分析手法』は、以下の通りである。
  - JIS9700:2013に記載されていないが、JIS9702:2000(JIS9700:2013へ統合)に記載されている。(HAZOPは記載されていない。)
  - また、ISO/TR 14121-2:2012にて、リスクアセスメントの各段階における数々の手法の実際的使用について示されている模様。(ISO/TR 14121-2:2012 については、未調査)

帰納的手法	両手法の使い分け	演繹的手法
PHA(予備危険源分析)	HAZOP(ハザード&オペラビリティー調査)	MOSAR法(系統的リスク分析のための組織化法)
ワット・イフ法		FTA(障害ツリー分析)
FMEA(故障モード及び影響分析)		デルファイテクニック

リスクの見積り

※参照：ISO12100

・ 個々の危険状態に関連するリスクは、危害の発生確率と危害の酷さとの組合せで表される。以降のスライドに、見積り基準を示す。

リスク(R) ＝ 危害の発生確率(P) × 危害の酷さ(S)
＝ (F + A + Ps) × S

以下の3点を考慮して、危害の発生確率(P)を求める。

■人の危険源への暴露(危険源にさらすこと)(F)
1)危険区域への接近の必要性
2)接近の性質
3)危険区域内での経過時間
3)接近者の数
5)接近の頻度

■危険事象の発生確率(Ps)
1)信頼性及び他の統計データ
2)事故履歴
3)健康障害履歴
4)リスク比較 ※

■危害の回避又は制限の可能性(A)
1)危険源に暴露される様々な人
2)危険状態から危害に至る早さ
3)リスクの認知
4)危害の回避又は制限にかかる人の能力
5)実際の経験及び知識

以下の2点を考慮して、危害の酷さ(S)を求める。

■障害又は健康障害の酷さ
1) 軽度
2) 重度
3) 死亡

■危害の範囲
1) 1人
2) 複数人

リスクの大きさの決定

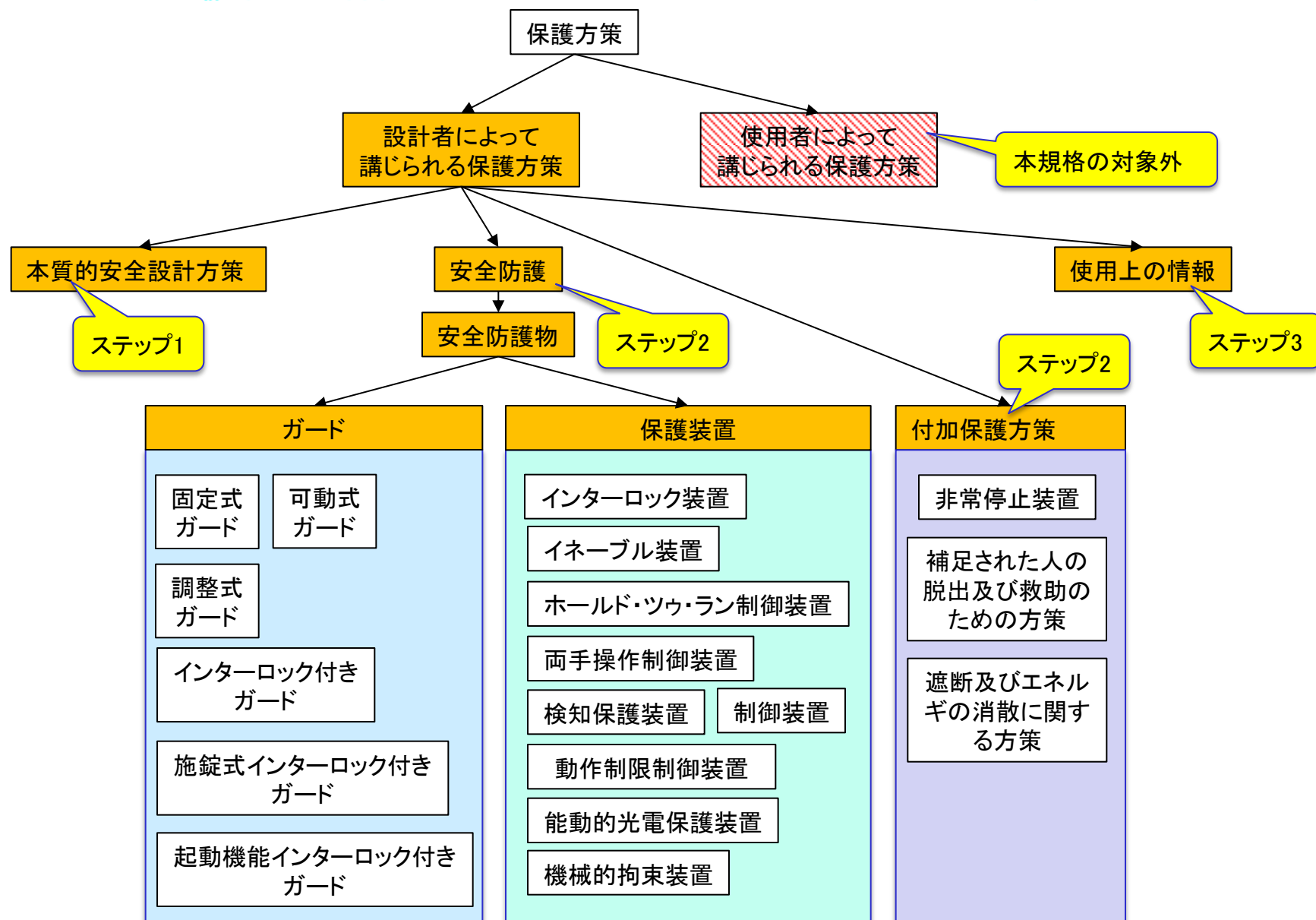
ISO26262 ASILの場合

※参照：ISO26262-5 表4

重篤度クラス	暴露頻度クラス	回避性クラス		
		C1	C2	C2
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

保護方策の種類

※参照：ISO12100

- 保護方策
  - 設計者によって講じられる保護方策
    - 本質的安全設計方策（ステップ1）
    - 安全防護（ステップ2）
      - 安全防護物
        - ガード
          - 固定式ガード
          - 可動式ガード
          - 調整式ガード
          - インターロック付きガード
          - 施錠式インターロック付きガード
          - 起動機能インターロック付きガード
        - 保護装置
          - インターロック装置
          - イネーブル装置
          - ホールド・ツゥ・ラン制御装置
          - 両手操作制御装置
          - 検知保護装置
          - 制御装置
          - 動作制限制御装置
          - 能動的光電保護装置
          - 機械的拘束装置
    - 付加保護方策（ステップ2）
      - 非常停止装置
      - 補足された人の脱出及び救助のための方策
      - 遮断及びエネルギの消散に関する方策
    - 使用上の情報（ステップ3）
  - 使用者によって講じられる保護方策（本規格の対象外）

3. セーフティの分析・設計技術（機能安全）

安全分析にて考慮すべき故障のパターン

株式会社ヴィッツ

- 系統的原因故障（バグ） と ランダムHW故障
- 単一故障 と 多重故障
  – IEC 61508では、単一故障のみ考慮
  – ISO 26262（自動車）では、２重故障まで考慮必要
  – BS EN 50129（鉄道）では、３重故障まで考慮必要
- 恒久故障 と 一時故障
  – 一時故障の例）ノイズによるメモリ化け
- 従属故障
  – ある故障が原因で、その影響を受け、別の箇所が故障する
- 共通原因故障
  – １つの原因により、複数箇所への同時故障が生じること
  – 例１）電源異常により、2マイコン共誤動作
  – 例2）ノイズの影響（環境）により、２マイコン共誤動作
  – 例3）安全系のある変数が化け、各出力系全てが誤動作
  – 例4）同一設計のソフトのため、同じ箇所にバグが存在

潜在故障

- 安全策（Safety Mechanism；SM）の潜在故障

a) 安全なケース

b) 危険なケース

対策例

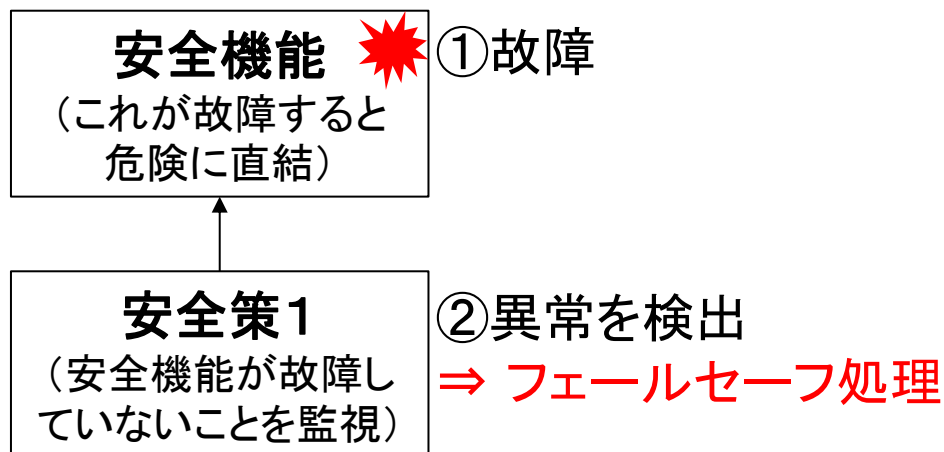
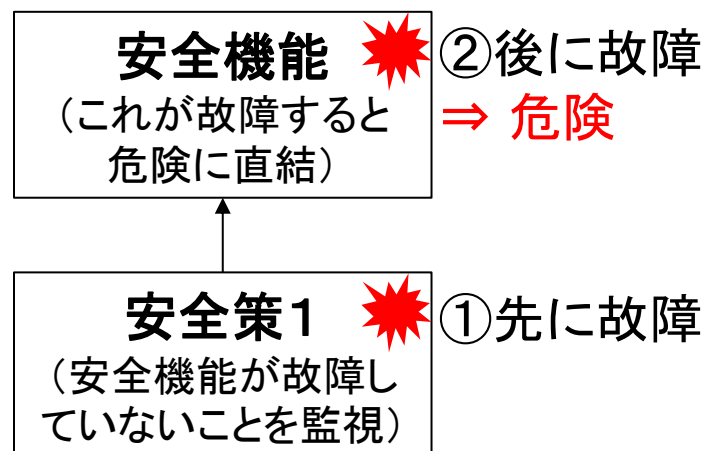
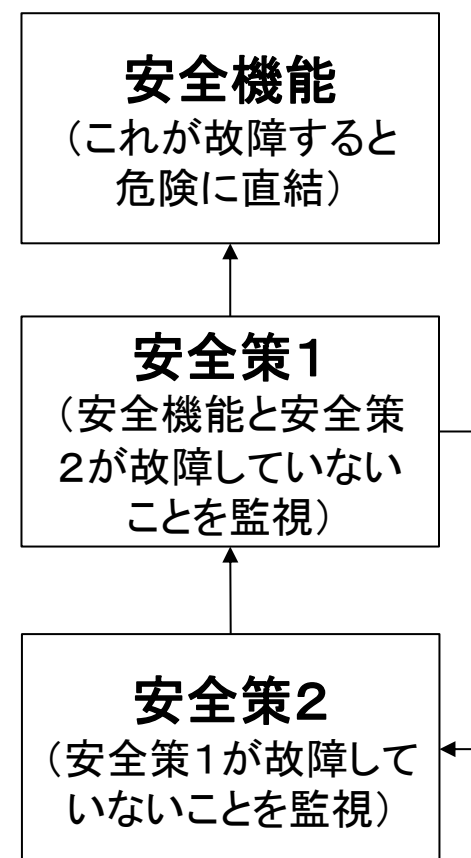
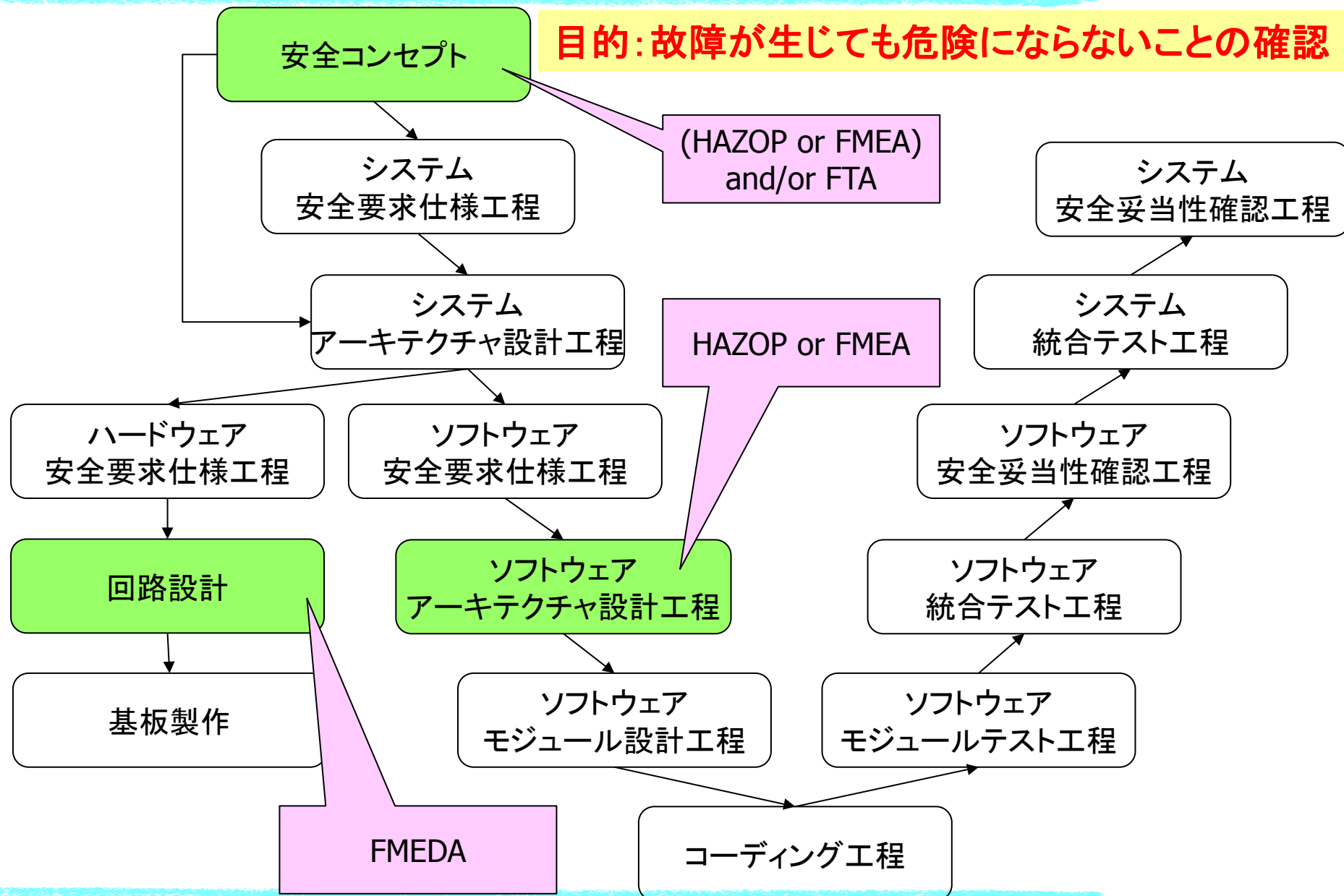
安全分析が必要な工程

目的:故障が生じても危険にならないことの確認

- 安全コンセプト
- システム 安全要求仕様工程
- システム アーキテクチャ設計工程
- ハードウェア 安全要求仕様工程
- ソフトウェア 安全要求仕様工程
- 回路設計
- 基板製作
- ソフトウェア アーキテクチャ設計工程
- ソフトウェア モジュール設計工程
- コーディング工程
- ソフトウェア モジュールテスト工程
- ソフトウェア 統合テスト工程
- ソフトウェア 安全妥当性確認工程
- システム 統合テスト工程
- システム 安全妥当性確認工程

(HAZOP or FMEA) and/or FTA

HAZOP or FMEA

FMEDA

ASILと安全策の例（RAM故障対策）

ISO26262-5 **Table D.6 — Volatile memory**

Safety mechanism/measure	See overview of techniques	Typical diagnostic coverage considered achievable **DC**	Notes
RAM pattern test	D.2.5.1	Medium **90%**	High coverage for stuck-at failures. No coverage for linked failures. Can be appropriate to run under interrupt protection
RAM March test	D.2.5.3	High **99%**	Depends on the write read order for linked cell coverage. Test generally not appropriate for run time
Parity bit	D.2.5.2	Low **60%**	—
Memory monitoring using error-detection-correction codes (EDC)	D.2.4.1	High **99%**	The effectiveness depends on the number of redundant bits. Can be used to correct errors
Block replication	D.2.4.4	High **99%**	Common failure modes can reduce diagnostic coverage
Running checksum/CRC	D.2.5.4	High **99%**	The effectiveness of the signature depends on the polynomial in relation to the block length of the information to be protected. Care needs to be taken so that values used to determine checksum are not changed during checksum calculation Probability is 1/maximum value of checksum if random pattern is returned

ソフトウェアにおける安全の確保方法

①厳密な機能安全プロセスでソフトウェアの開発を行う。

②システムレベルで導き出されたソフトウェアの技術的な安全策について、詳細レベルで十分であるかを確認する。不足している場合、新たな安全策を追加する。

ソフトウェアにおける主な安全策

故障モード	主な安全策	ISO26262-5
ROM故障	・チェックサムやCRCによるROM故障検出	Table D.5
RAM故障	・チェックサムやパターンテストによるRAM故障検出 ・安全関連データの2重管理	Table D.6
CPUコア故障	・レジスタのテスト ・スタックオーバー／アンダーフロー検出	Table D.4
クロック故障	・タイムウインド付きWDT	Table D.10
内部バス故障検出	・ウォーキングビットによるバス故障検出	Table D.14
ソフトウェアの誤動作	・実行シーケンスモニタ＋WDT	Table D.10

ソフトウェアのバグ（誤動作）検出機構

ISO26262-6 **Table 4 — Mechanisms for error detection at the software architectural level**

	Methods	ASIL A	ASIL B	ASIL C	ASIL D
1a	Range checks of input and output data	++	++	++	++
1b	Plausibility check[a]	+	+	+	++
1c	Detection of data errors[b]	+	+	+	+
1d	External monitoring facility[c]	o	+	+	++
1e	Control flow monitoring	o	+	++	++
1f	Diverse software design	o	o	+	++

＜従来開発＞

テストがしっかり出ていてバグが無い。

＜機能安全＞

テストの完全性は不可能。

バグが潜んでいることを前提に対処。

4. セーフティの立証技術

安全ケース(Safety case)

- 安全ケースとは、アイテムに対する安全要求が完全であり、かつ、満足されているということを、開発における安全活動の成果物からまとめたエビデンスによって主張すること
- 目的:
  - 安全ケースは、特定のコンテキストで運用されるシステムが、非合理的なリスクを伴わないということの、明確で包括的でディフェンス可能な(エビデンスに基づく)主張を伝える。
- 主要な3要素
  - 要求事項
  - アーギュメント
  - エビデンス

(第10部5.3「安全ケースの理解」より)

GSNでSafety Caseの目次を表現

- GSN ＝ Goal Structuring Notation
  - 安全などの「主張」と、それを支持する「議論」の構造を表す図。
- Safety CaseのTOP（目次）をGSNで表す。
- GSNの末端のSolutionから、具体的な開発成果物へのリンクを貼り、全ての成果物の紐付けを行う。

G1
C/S Logic is fault free

S1
Argument by satisfaction of all C/S safety requirements

S2
Argument by omission of all identified software hazards

C1
Identified software hazards

G2
Press controls being 'jammed on' will cause press to halt

G3
Release of controls prior to press passing physical PoNR will cause press operation to abort

G4
C/S fails safe (halts) on, and annunciates (by sounding klaxon), all single component failures

G8
Unintended opening of press (after PoNR) can only occur as a result of component failure

G9
Unintended closing of press can only occur as a result of component failure

Sn1
Black Box Test Results

G5
'Failure1' transition of PLC state machine includes BUTTON_IN remaining true

G7
'Abort' transition of PLC state machine includes BUTTON_IN going FALSE

Sn3
Fault tree analysis cutsets for event 'Hand trapped in press due to command error'

Sn4
Hazard directed test results

Sn2
C/S State Machine

Figure 5 – An Example Goal Structure

※抜粋元：
http://www-users.cs.york.ac.uk/tpk/dsn2004.pdf

System can tolerate single component failures

Goal

Fault Tree for Hazard H1

Solution

Argument by elimination of all hazards

Strategy

All Identified System Hazards

Context

Undeveloped Goal (to be developed further)

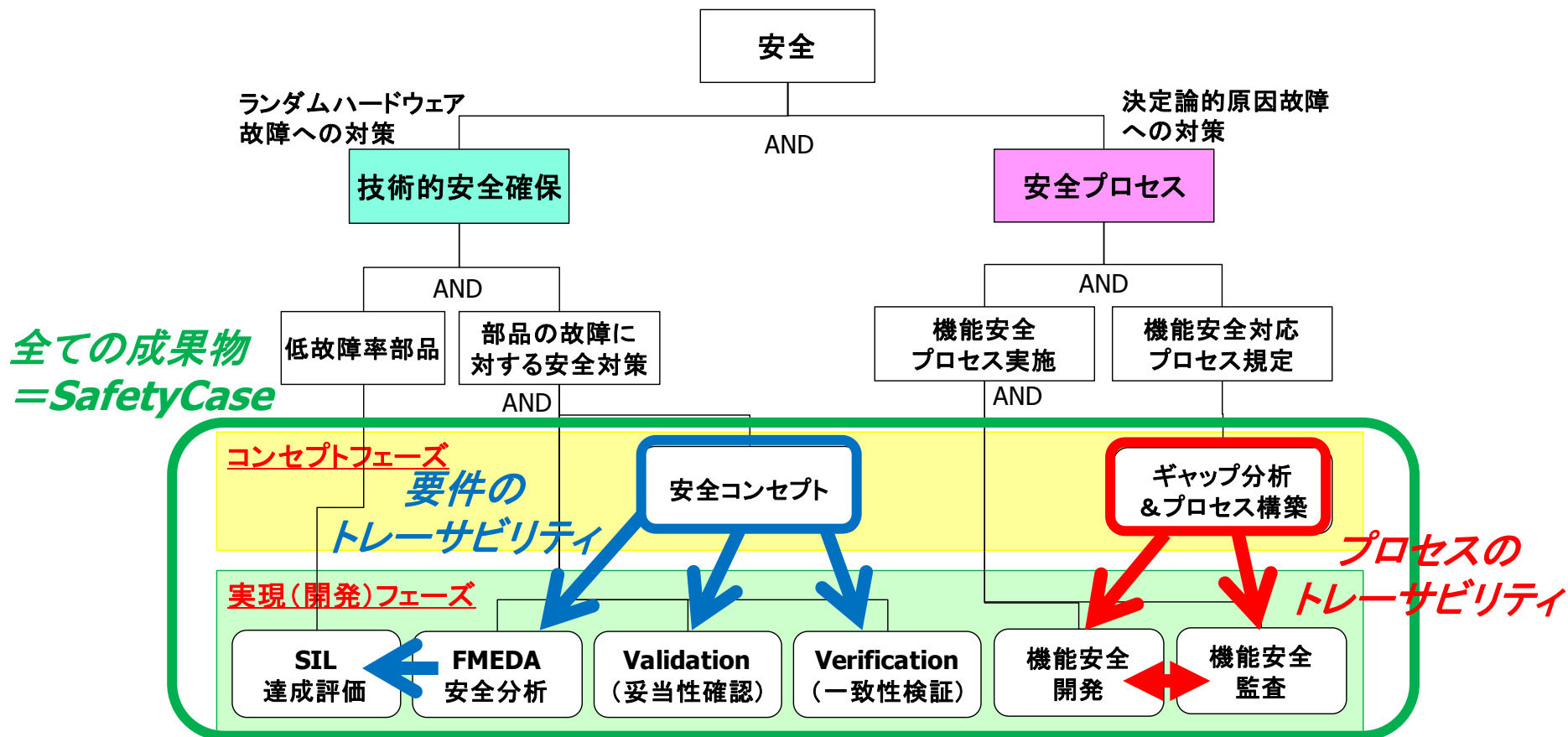
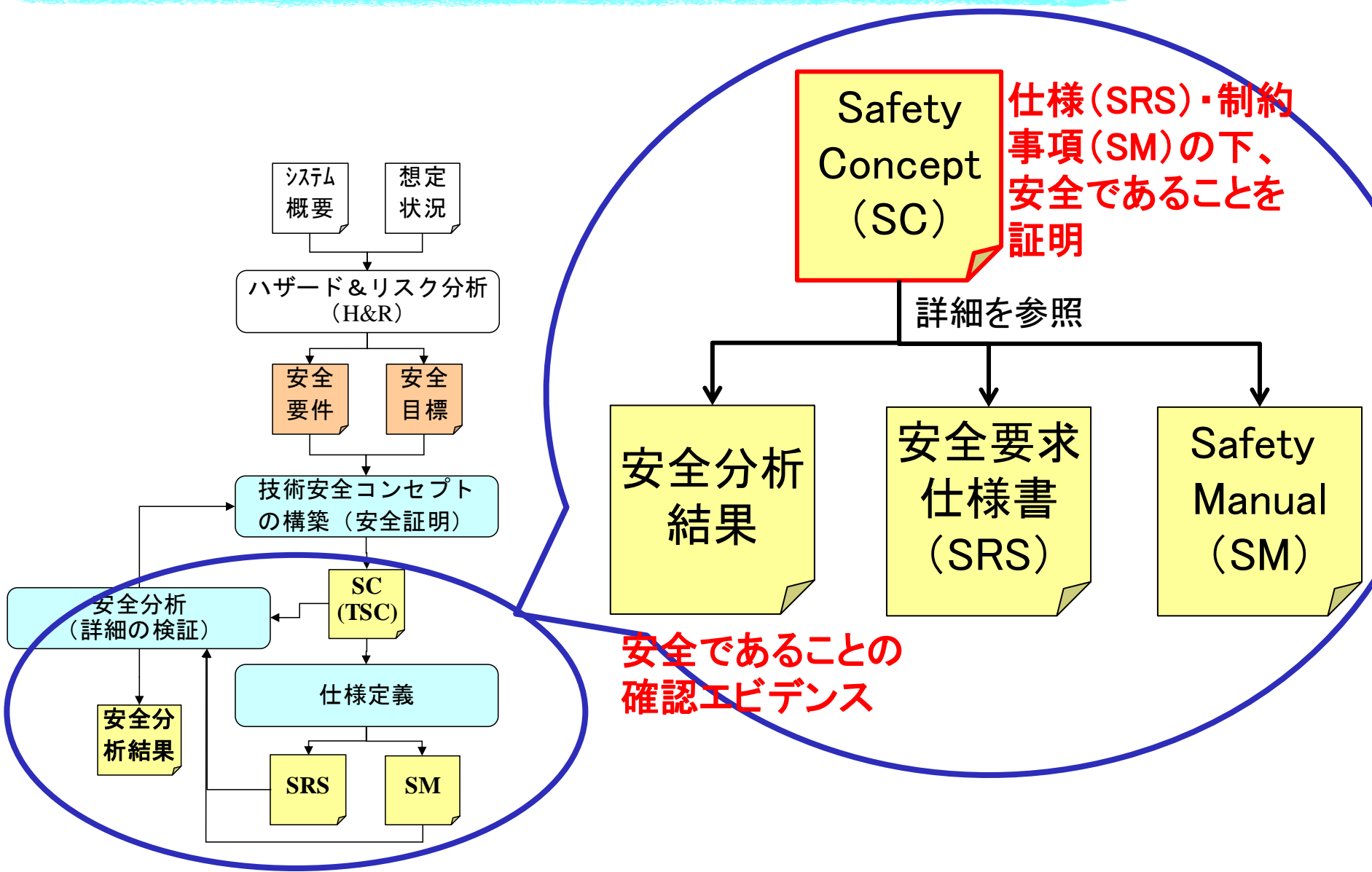
Figure 4- Principal Elements of the Goal Structuring Notation

※注）実際は、あらゆる成果物が紐付くレベルの、詳細なGSNになる。

成果物一式でSafety Caseを主張

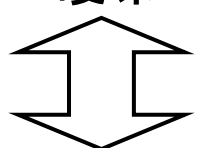
- その場合、
  - 技術的なTOP文書：技術安全コンセプト
  - プロセスのTOP文書：機能安全対応プロセス規定／認証取得済プロセス規定
- 各TOP文書からのトレースがとれていることが重要！！

【弊社事例】技術安全コンセプト4文書による立証

「可読性」の向上 ～準形式手法～

機能安全では、準形式手法を推奨

ISO26262-6 Table 2 — Notations for software architectural design

客観的に曖昧

明確

	Methods		ASIL A	ASIL B	ASIL C	ASIL D
1a	Informal notations	独自の図	++	++	+	+
1b	Semi-formal notations	フォーマットが決められた図（UMLなど）	+	++	++	++
1c	Formal notations	形式記述	+	+	+	+

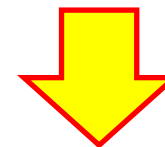
詳細

IEC61508-3:2010

Table B.7 – Semi-formal methods

(Referenced by Tables A.1, A.2 and A.4)

	Technique/Measure *		Ref	SIL 1	SIL 2	SIL 3	SIL 4
1	Logic/function block diagrams	ブロック間I/F	See Note 1	R	R	HR	HR
2	Sequence diagrams	シーケンス	see Note 1	R	R	HR	HR
3	Data flow diagrams	データ	C.2.2	R	R	R	R
4a	Finite state machines/state transition diagrams	状態	B.2.3.2	R	R	HR	HR
4b	Time Petri nets	時間＋状態	B.2.3.3	R	R	HR	HR
5	Entity-relationship-attribute data models	関連	B.2.4.4	R	R	R	R
6	Message sequence charts	通信	C.2.14	R	R	R	R
7	Decision/truth tables	条件	C.6.1	R	R	HR	HR
8	UML		C.3.12	R	R	R	R

従来：
様々な観点で設計

機能安全：
様々な観点を
わかりやすく図示

「可読性」の向上 ～文書品質の改善～
システム開発文書品質研究会(ASDoQ)

文書品質が低いと多大な問題が生じます!!

- 開発工程間の手戻りが発生 ⇒コスト増加
- テスト設計が要求に基づいていない ⇒欠陥の検出不可
- テストが場当たり的 ⇒欠陥の検出不可
- 実装が設計からかけ離れている ⇒欠陥の混入
- バグ修正や仕様変更する場所がわからない ⇒保守できない
- 取扱説明書が頼りにならない ⇒誤使用による危険発生

開発者　ユーザ

種別	任意団体
会員	団体、個人
会費	原則無料
条件	ASDoQ 著作物の取り扱いへの合意 著作権は、著作者に属する 著作者は、著作物の使用・複製・改変・再配布を認める
シンポジウム	1回/年の頻度で開催
研究会	3-4回/年の頻度で開催
作業部会	必要に応じて設立し随時開催

【入会申込・お問合せ先】
システム開発文書品質研究会　http://asdoq.jp/
secretariat@asdoq.jp (ASDoQ事務局)
(事務局所在地)
名古屋大学 情報科学研究科附属組込みシステム研究センター内

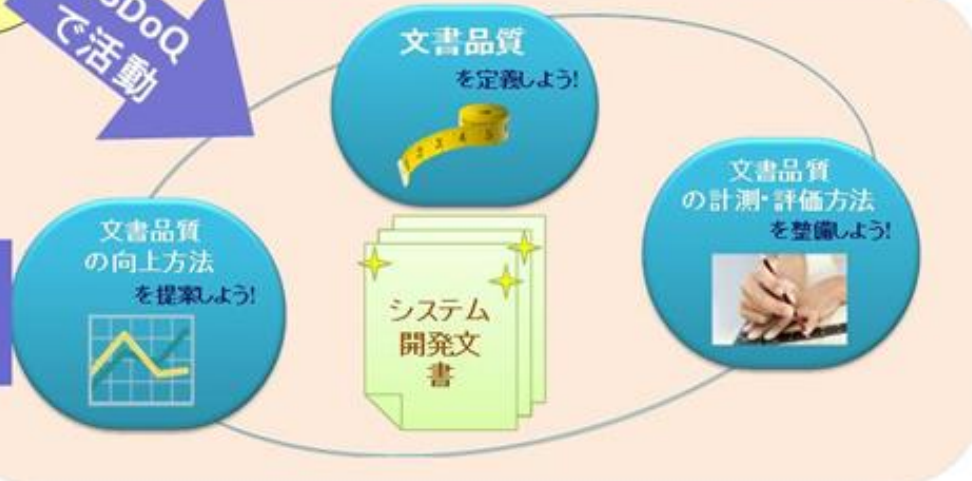
ASDoQで活動

- 文書品質を定義しよう!
- 文書品質の計測・評価方法を整備しよう!
- 文書品質の向上方法を提案しよう!
- システム開発文書

研究成果(予定)

主な成果物

- 開発文書の品質の定義
- 開発文書品質の計測方法
- 開発文書品質の向上方法
- 品質の高い開発文書例

要件のトレーサビリティ管理方法

- **要求番号の付与粒度は文章単位（認証機関指摘事項）**
- 上流文書との紐付を手作業で実施する必要あり（膨大な作業量）
  - **どんな優れたツールを用いても回避不可能！**

【NG事例】章番号単位で番号付与 → **【OK事例】文章単位で番号付与**

【NG事例】

6.2.4.2.　処理単位の実行順序[OS-SW-02-REQ-00058:　OS-SW-02-REQ-00001]

処理単位の実行順序を規定するために、ここでは、処理単位の優先順位を規定する。また、ディスパッチが起こるタイミングを規定するために、ディスパッチを行うカーネル内の処理であるディスパッチャの優先順位についても規定する。

タスクの優先順位は、ディスパッチャの優先順位よりも低い。タスク間では、高い優先度を持つ方の優先順位が高く、同じ優先度を持つタスク間では、先に実行できる状態となった方の優先順位が高い。詳しくは、「6.2.6.2タスクスケジューリング規則」の節を参照すること。

割込みハンドラの優先順位は、ディスパッチャの優先順位よりも高い。割込みハンドラ間では、高い割込み優先度を持つ方が優先順位が高く、同じ割込み優先度を持つ割込みハンドラ間では、先に実行開始された方が優先順位が高い。同じ割込み優先度を持つ割込みハンドラ間での実行開始順序は、この仕様では規定しない。詳しくは、「6.2.7.2割込み優先度」の節を参照すること。

割込みサービスルーチンとタイムイベントハンドラの優先順位は、それを呼び出す割込みハンドラと同じである。

CPU例外ハンドラの優先順位は、CPU例外がタスクで発生した場合には、ディスパッチャの優先順位と同じであるが、ディスパッチャよりも先に実行される。CPU例外がその他の処理単位で発生した場合には、CPU例外ハンドラの優先順位は、その処理単位の優先順位と同じであるが、その処理単位よりも先に実行される。

初期化ルーチンは、カーネルの動作開始前に、システムコンフィギュレーションファイル中に初期化ルーチンを登録する静的APIを記述したのと同じ順序で実行される。終了処理ルーチンは、カーネルの動作終了後に、終了処理ルーチンを登録する静的APIを記述したのと逆の順序で実行される。

【OK事例】

6.2.4.2.　処理単位の実行順序

処理単位の実行順序を規定するために、ここでは、処理単位の優先順位を規定する。また、ディスパッチが起こるタイミングを規定するために、ディスパッチを行うカーネル内の処理であるディスパッチャの優先順位についても規定する。

タスクの優先順位は、ディスパッチャの優先順位よりも低い[OS-SW-02-REQ-00058: OS-SW-02-REQ-00001]。タスク間では、高い優先度を持つ方の優先順位が高く、同じ優先度を持つタスク間では、先に実行できる状態となった方の優先順位が高い[OS-SW-02-REQ-00059: OS-SW-02-REQ-00001]。詳しくは、「6.2.6.2タスクスケジューリング規則」の節を参照すること。

割込みハンドラの優先順位は、ディスパッチャの優先順位よりも高い[OS-SW-02-REQ-00060: OS-SW-02-REQ-00001]。割込みハンドラ間では、高い割込み優先度を持つ方が優先順位が高く、同じ割込み優先度を持つ割込みハンドラ間では、先に実行開始された方が優先順位が高い[OS-SW-02-REQ-00061: OS-SW-02-REQ-00001]。同じ割込み優先度を持つ割込みハンドラ間での実行開始順序は、この仕様では規定しない。詳しくは、「6.2.7.2割込み優先度」の節を参照すること。

割込みサービスルーチンとタイムイベントハンドラの優先順位は、それを呼び出す割込みハンドラと同じである。

CPU例外ハンドラの優先順位は、CPU例外がタスクで発生した場合には、ディスパッチャの優先順位と同じであるが、ディスパッチャよりも先に実行される[OS-SW-02-REQ-00062: OS-SW-02-REQ-00001]。CPU例外がその他の処理単位で発生した場合には、CPU例外ハンドラの優先順位は、その処理単位の優先順位と同じであるが、その処理単位よりも先に実行される[OS-SW-02-REQ-00063: OS-SW-02-REQ-00001]。

初期化ルーチンは、カーネルの動作開始前に、システムコンフィギュレーションファイル中に初期化ルーチンを登録する静的APIを記述したのと同じ順序で実行される[OS-SW-02-REQ-00064: OS-SW-02-REQ-00001]。終了処理ルーチンは、カーネルの動作終了後に、終了処理ルーチンを登録する静的APIを記述したのと逆の順序で実行される[OS-SW-02-REQ-00065: OS-SW-02-REQ-00001]。

※当社製機能安全RTOSの安全要求仕様書からの抜粋
※赤字は要求番号

厳格なレビューの実施：レビューの種類

- **ピアレビュー**
  - 作成した開発文書の中身に誤りが無いかを、同僚やチームメンバーがチェックすること。非公式レビューの一種。
  - **第3者観点が欠落するため、開発時の思い込みミスや、非可読性に関する検出が弱い。**
- **ウォークスルー**
  - 開発文書の中身に誤りが無いかを、複数人で集まりチェックすること。公式レビューの一種。
  - レビュア：開発の専門家、ターゲットシステムの専門家、品質の専門家、安全の専門家。
- **インスペクション**
  - 開発文書の中身に誤りが無いかを、複数人でチェックすること。公式レビューの一種。
  - レビュア：開発の専門家、ターゲットシステムの専門家、品質の専門家、安全の専門家。**文書作成者は参加できない。**
  - **各レビューは事前レビューを実施する必要あり。**
  - 事前レビューと、合同レビューの２段階実施する。

機能安全で要求される高い説明力が必要!!

レビューの完全性

・各開発工程（アーキテクチャ設計工程、モジュール設計工程、実装、単体テスト、統合テスト、・・・）にてゲートが必要。

・ゲートでは、厳密なレビューとエビデンス（記録）が必要。

レビュー内容が本当に正しいことを説明できる文書化が必要。
（従来の指摘事項の記録だけではNG）

1ページ

※当社の認証プロセスの例

トレーサビリティツール活用による効率化

	上位の要求番号	上位の要求内容	下位の要求番号	下位の要求内容	レビュア名	レビュー評価	レビュー内容
1	OS-SW-01-REQ-0	指定されたブロックに対して以下の処理を実施する。	OS-SW-02-VAS-0	テスト手順「ROM2 No.5, 11」を満たす内容であること。タイマ等を用いて、即割込みを発生させる。割込みが発生するまでの時間以上をループ等で待つ。割込みは発生しない。	中野 泰伸	OK	問題なし
2	OS-SW-01-REQ-0	コールバック関数呼び出し時の割込み禁止/許可状態は、全割込み禁止状態とする。	OS-SW-02-VAS-0	テスト手順「ROM2 No.5, 11」を満たす内容であること。タイマ等を用いて、即割込みを発生させる。割込みが発生するまでの時間以上をループ等で待つ。割込みは発生しない。	中野 泰伸	NG	
3	OS-SW-03-DSN-0	romck_chk_ablkの決定表	OS-SW-02-VAS-0	テスト手順「ROM2 No.5, 11」を満たす内容であること。タイマ等を用いて、即割込みを発生させる。割込みが発生するまでの時間以上をループ等で待つ。割	中野 泰伸	OK	問題なし
4	OS-SW-03-DSN-0	romc 決定				未検討	
5	OS-SW-03-DSN-0	romc 決定					

①同時に複数文書間の内容を確認

	B	C	D	E	F	G	H	I
1	上位の要求番号	上位の要求内容	ドキュメント名	下位の要求番号	下位の要求内容	レビュア名	レビュー評	レビュー内容
2			OS-SW-01-R	OS-SW-01-REQ-	IEC 61508の第2部の表	浅野	OK	問題なし
3	OS-SW-01-REQ-02043	IEC 61508の第2部	OS-SW-01-R	OS-SW-01-REQ-	ROMの故障検出チェック	浅野	OK	問題なし
4	OS-SW-01-REQ-02043	IEC 61508の第2部	OS-SW-01-R	OS-SW-01-REQ-	ROMの故障検出チェック	浅野	OK	問題なし
5	OS-SW-01-REQ-02043	IEC 61508の第2部	OS-SW-01-R	OS-SW-01-REQ-	CRC生成多項式として、	浅野	OK	
6	OS-SW-01-REQ-02043	IEC 61508の第2部	OS-SW-01-R	OS-SW-01-REQ-	電源投入時及びリセット	浅野	OK	
7	OS-SW-01-REQ-02043	IEC 61508の第2部	OS-SW-01-R	OS-SW-01-REQ-	ランタイム時･･･1ブロック	浅野	OK	
8	OS-SW-01-REQ-02050	電源投入時及びリ	OS-SW-01-R	OS-SW-01-REQ-	電源投入時及びリセット	浅野	OK	
9	OS-SW-01-REQ-02046	ROMの故障検出チ	OS-SW-01-R	OS-SW-01-REQ-	ブロック毎に、以下の処	浅野	未検討	
10	OS-SW-01-REQ-02047	ROMの故障検出チ	OS-SW-01-R	OS-SW-01-REQ-	ブロック毎に、以下の処	浅野	未検討	
11	OS-SW-01-REQ-02049	CRC生成多項式と	OS-SW-01-R	OS-SW-01-REQ-	ブロック毎に、以下の処	浅野	未検討	
12	OS-SW-01-REQ-02052	電源投入時及びリ	OS-SW-01-R	OS-SW-01-REQ-	ブロック毎に、以下の処	浅野	未検討	
13	OS-SW-01-REQ-02055	ブロック毎に、以下	OS-SW-01-R	OS-SW-01-REQ-	コールバック関数呼び出	浅野	未検討	
14	OS-SW-01-REQ-02055	ブロック毎に、以下	OS-SW-01-R	OS-SW-01-REQ-	また、コールバック関数	浅野	未検討	
15	OS-SW-01-REQ-02059	指定されたブロック	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM2 No.5,	泉	OK	問題あり
16	OS-SW-01-REQ-02059	指定されたブロック	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM2 No.5,	中野泰伸	OK	問題なし
17	OS-SW-01-REQ-02234	コールバック関数	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM2 No.5,	中野泰伸	NG	問題あり
18	OS-SW-01-REQ-02234	コールバック関数	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM2 No.5,	泉	未検討	
19	OS-SW-03-DSN-00583	romck_chk_ablkの	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM2 No.5,	泉	未検討	
20	OS-SW-03-DSN-00583	romck_chk_ablkの	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM2 No.5,	中野泰伸	OK	検討の必要あり
21	OS-SW-03-DSN-00583	romck_chk_ablkの	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM6 No.7,	中野泰伸	OK	テスト
22	OS-SW-03-DSN-00583	romck_chk_ablkの	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM6 No.7,	泉	未検討	
23	OS-SW-03-DSN-00583	romck_chk_ablkの	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM6 No.2	泉	未検討	
24	OS-SW-03-DSN-00583	romck_chk_ablkの	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM6 No.2	中野泰伸	未検討	
25	OS-SW-03-DSN-00583	romck_chk_ablkの	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM6 No.1,	泉	未検討	
26	OS-SW-03-DSN-00583	romck_chk_ablkの	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM6 No.1,	中野泰伸	未検討	
27	OS-SW-03-DSN-00584	romck_cal_crcの決	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM3 No.1,	中野泰伸	未検討	
28	OS-SW-03-DSN-00584	romck_cal_crcの決	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM3 No.1,	泉	未検討	
29	OS-SW-01-REQ-02265	具体的な動作は	OS-SW-08-T	OS-SW-02-VAS-	テスト手順「ROM6 No.2	中野泰伸	未検討	

②そのままレビュー結果を記録

③複数人のレビュ結果をマージしインスペクションレビュー活用

影響分析も同様に実施

本ツールの画面：当社製トレーサビリティ管理ツール“Greyhound ”より
平成21年度 全国中小企業団体中央会 試作開発等支援事業にて開発

5. ガイドブックのご紹介

ガイドブックのセーフティ設計関連 目次(仮)

SEC BOOKS:
品質向上のためのセーフティ&セキュリティ設計の勧め(仮)

※ガイドブック発刊に向けて、IPA/SECにて現在取りまとめ中です。
※下記目次は、サプライチェーンにおける品質の見える化WG検討資料より一部抜粋。

- セーフティのためのソフトウェア設計
  - ➢ セーフティ設計の開発プロセス
    - ➢ セーフティを考慮した設計とは
    - ➢ セーフティを考慮したソフトウェア開発プロセス
  - ➢ セーフティ設計の手法
    - ハザード&リスク分析
    - セーフティを実現するための技術
      - ✓ セーフティに有効な設計手法
      - ✓ 安全性を高める考え方
  - ➢ セーフティ設計の評価手法と認証
    - セーフティ設計の妥当性確認
    - 機能安全認証

ご清聴ありがとうございました。

本内容の関連サイトもご覧ください。
◎当社ホームページ：http://www.witz-inc.co.jp/
◎TÜV SÜD による認証確認サイト：
http://www.tuev-sued.de/industry_and_consumer_products/certificates
（Search欄で、"Witz Corporation"と入力してください）
◎プロセス認証プレス発表記事
日本経済新聞：http://release.nikkei.co.jp/detail.cfm?relID=306435&lindID=1
EDN：http://ednjapan.com/edn/articles/1203/29/news083.html
Tech On!：http://techon.nikkeibp.co.jp/article/NEWS/20120329/210429/
パナソニック：http://panasonic.co.jp/corp/news/official.data/data.dir/jn120329-8/jn120329-8.html
東芝：http://www.toshiba.co.jp/about/press/2012_03/pr_j2901.htm
iPROS：http://www.ipros.jp/news/article/detail/3649/
Response：http://response.jp/article/2012/03/30/172177.html
Tech-On!（IEC61508）：http：//techon.nikkeibp.co.jp/article/NEWS/20100512/182502/

本内容についてのご質問は下記にお願いします

株式会社ヴィッツ 執行役員
機能安全開発部 部長　森川 聡久
morikawa@witz-inc.co.jp
Tel: 052-220-1218